

Appln. No. 09/435,736

Attorney Docket No. 4366-41

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

**In re Patent Application for:**  
Avaya Technology Corp.

**Art Unit:** 2137

**First Named Inventor:** REISMAN, Arthur

**Examiner:** NGUYEN, M.

**Appln. No.:** 09/435,736

**Confirmation No.:** 5609

**Filing Date:** November 8, 1999

**For:** Encrypted and Non-Encrypted Communication  
of Message Data

\* \* \*

**APPELLANTS' BRIEF**

MS Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

Appellants hereby appeal to the Board of Appeals in response to the Notice of Panel Decision from Pre-Appeal Brief Review of July 9, 2007. The fee set forth in 37 CFR § 41.20(b) has been previously submitted in connection with the Request for Pre-Appeal Brief Request for Review. Although Appellants believe that no additional fees are due at this time, authorization to charge any necessary fees to Deposit Account No. 19-1970 is hereby given.

A single copy of this Appeal Brief is being submitted pursuant to MPEP § 1205.02.

(i) REAL PARTY IN INTEREST

All right, title, and interest in this application has been assigned to Avaya Technology Corp. This Assignment is recorded at Reel/Frame 012707/0562.

(ii) RELATED APPEALS AND INTERFERENCES

There are no related appeals, interferences or judicial proceedings known to Appellants, or the Appellants' legal representative which may be related to, directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal.

(iii) STATUS OF CLAIMS

Claims 2-11, 13, 14, 16-24 and 26-45 are pending in the application, with all claims being appealed.

Claims 2-4, 6, 13, 16-18, 20, 23, 26, 30 and 24 are objected to. Appellants agree with the Examiner's interpretation of these claims and for purposes of this Appeal would like those claims interpreted consistent with ¶ 4 of the March 23, 2007 Office Action.

Claims 28 and 39 are rejected under 35 U.S.C. §101.

Claims 4-5, 10-11, 18-19, 23-24, 26-30, 32-35 and 44-45 are rejected under 35 U.S.C. §102(e).

Claims 2, 13-14, 16, 31 and 36-43 are rejected under 35 U.S.C. §103(a).

Claims 3 and 17 are rejected under 35 U.S.C. §103(a).

Claims 6, 8-9 and 21-22 are rejected under 35 U.S.C. §103(a).

Claims 7 and 20 are rejected under 35 U.S.C. §103(a).

The Pending Claims are set forth in the CLAIMS APPENDIX.

(iv) STATUS OF AMENDMENTS

No Amendments have been filed subsequent to the March 6, 2006 Office Action.

(v) SUMMARY OF CLAIMED SUBJECT MATTER

**Independent Claim 36** is directed toward a method of communication data between a first computing device and a second computing device, the method comprising: (See pg. 2, last paragraph bridging to pg. 3)

(a) a browser on the first computing device providing a Web page to a user, the Web page comprising at least first and second input fields for input from the user and at least a first presentation field associated with the at least first and second input fields and wherein the Web page displays, simultaneously to the user, the first and second input fields; (See Fig. 2 and Pg. 7, last paragraph bridging to pg. 3)

(b) a program on the first computing device receiving a message from the user, wherein the message comprises at least a first and second datum input by the user into the at least first and second input fields, respectively, of the Web page, wherein the first datum is confidential to the user and the second datum is non-confidential to the user, and wherein the first datum comprises at least one of a credit card number and a social security number; (See pg. 3, pg. 4, top of pg. 7, first full paragraph, pg. 10, pg. 11 and Fig. 2)

(c) the program identifying that the first datum is confidential and the second datum is non-confidential; (See pg. 3, pg. 4, top of pg. 7, first full paragraph, pg. 10, pg. 11 and Fig. 2)

(d) the first computing device communicating, to the second computing device over an untrusted network, the first datum with encryption; and (See top of pg. 3)

(e) the first computing device communicating, to the second computing device over the untrusted network, the second datum without encryption, wherein steps (d) and (e) occur at least substantially simultaneously. (See top of pg. 3 and Abstract)

**Independent Claim 40** is directed toward a system for communicating data between first and second computing devices, comprising: (See pg. 2, last paragraph bridging to pg. 3)

(a) a first computer device operable to communicate data over an untrusted network, the first computer device comprising:

a user display, the display comprising, at one time, at least first and second input fields of a Web page for input from the user and at least a first presentation field associated with the at least first and second input fields; (See Fig. 2)

means for receiving input information from the user, wherein the information comprises at least a first and second datum input by the user into the at least first and second input fields, respectively, of the display, wherein the first datum is confidential to the user and the second datum is non-confidential to the user, wherein the first datum comprises at least one of a credit card number and a social security number; and (See pg. 3, last paragraph bridging to pg. 4, pg. 10, first full paragraph and Figs. 1-2)

means for identifying that the first datum is confidential and the second datum is non-confidential; and (See pgs. 2-4, pg. 7, first paragraph, and Fig. 1)

(b) a second communication device in communication with the first communication device, wherein the first computing device communicates, to the second computing device over the untrusted network, the first datum with encryption and the second datum without encryption. (See pg. 2, last paragraph bridging to pg. 3)

**Independent Claim 44** is directed toward a method of communicating data between a first computing device and a second computing device, the method comprising the steps of: (See pg. 2, last paragraph bridging to pg. 3)

at a first computing device, receiving input information from one Web page displayed to a user, the input information comprising at least first and second datum corresponding respectively to at least first and second user input fields, wherein the first datum comprises at least one of a credit card number and a social security number; (See pg. 2, last paragraph bridging to pg. 3, and first full paragraph, pg. 3)

at the first computing device, a program determining which of the at least first and second user input fields contains confidential information, wherein the first datum is confidential to the user and the second datum is not confidential to the user; (See pg. 7, first full paragraph)

the first computing device communicating the first datum to a second computing device over an untrusted network with encryption of the first datum; and (See pg. 11, lines 5-10)

the first computing device communicating the second datum over the untrusted network to the second computing device without encryption of the second datum. (See pg. 11, lines 5-10 and lines 15-20)

**Independent Claim 45** is directed toward a data communication system, comprising:

a first computer device operable to communicate data over an untrusted network, the first computer device comprising: (See pg. 3, lines 4-12 and Fig. 1)

(a) a user display, the display comprising at least first and second input fields of a single, displayed Web page for input from the user and at least a first presentation field associated with the at least first and second input fields; (See Fig. 2 and Pg. 7, last paragraph bridging to pg. 3)

(b) an input operable to receive input information from the user, wherein the information comprises at least a first and second datum input by the user into the at least first and second input fields, respectively, of the display, wherein the first datum is confidential to the user and the second datum is non-confidential to the user, and wherein the first datum comprises at least one of a credit card number and a social security number; and (See pgs 10-11 and Figs 1-2)

(c) a procedure operable to identify that the first datum is confidential and the second datum is non-confidential; (See pg. 11, lines 5-10)

wherein a second communication device is in communication with the first communication device and wherein the first computing device communicates, to the second computing device over the untrusted network, the first datum with encryption and the second datum without encryption. (See Fig. 1 and pg.7, first two paragraphs)

(vi) GROUND OF REJECTION TO BE REVIEWED ON APPEAL

Whether Claims 28 and 39 are in compliance with 35 U.S.C. §101.

Whether claims 4-5, 10-11, 18-19, 23-24, 26-30, 32-35 and 44-45 are anticipated by Saliba (U.S. Patent 6,052,710) under 35 U.S.C. §102(e).

Whether claims 2, 13-14, 16, 31 and 36-43 are obvious under 35 U.S.C. §103(a) in view of Saliba and Ice (U.S. Patent 6,589,031).

Whether claims 3 and 17 are obvious under 35 U.S.C. §103(a) in view of Saliba and Trcka (U.S. Patent Publication 2001/0039579).

Whether claims 6, 8-9 and 21-22 are obvious under 35 U.S.C. §103(a) in view of Saliba and Schneier.

Whether claims 7 and 20 are obvious under 35 U.S.C. §103(a) in view of Saliba and Chang (U.S. Patent 6,105,021).

(vii) ARGUMENT

**Whether claims 4-5, 10-11, 18-19, 23-24, 26-30, 32-35 and 44-45 are anticipated by Saliba (U.S. Patent 6,052,710) under 35 U.S.C. §102(e).**

Independent Claim 44 recites a method of communicating data between a first computing device and a second computing device, the method comprising the steps of:

at a first computing device, receiving input information from one Web page displayed to a user, the input information comprising at least first and second datum corresponding respectively to at least first and second user input fields, wherein the first datum comprises at least one of a credit card number and a social security number;

at the first computing device, a program determining which of the at least first and second user input fields contains confidential information, wherein the first datum is confidential to the user and the second datum is not confidential to the user;

the first computing device communicating the first datum to a second computing device over an untrusted network with encryption of the first datum; and

the first computing device communicating the second datum over the untrusted network to the second computing device without encryption of the second datum.

Independent Claim 45 recites a data communication system, comprising:

a first computer device operable to communicate data over an untrusted network, the first computer device comprising:

(a) a user display, the display comprising at least first and second input fields of a single, displayed Web page for input from the user and at least a first presentation field associated with the at least first and second input fields;

(b) an input operable to receive input information from the user, wherein the information comprises at least a first and second datum input by the user into the at least first and second input fields, respectively, of the display, wherein the first datum is confidential to the user

and the second datum is non-confidential to the user, and wherein the first datum comprises at least one of a credit card number and a social security number; and

(c) a procedure operable to identify that the first datum is confidential and the second datum is non-confidential;

wherein a second communication device is in communication with the first communication device and wherein the first computing device communicates, to the second computing device over the untrusted network, the first datum with encryption and the second datum without encryption.

As discussed in accordance with an exemplary embodiment in the specification, the entry (input) fields allow a user to input characters or text. These entry (input) fields are portions of a web page that can include, for example, a number of entry fields and a number of presentation fields. (See, for example, pgs. 7 and 8 of Appellants specification.) An embedded program encrypts confidential data provided by a user without encrypting non-confidential data provided by a user. (See top of pg. 7)

Independent claims 44 and 45 include either a program or procedure that identifies that the first datum is confidential and the second datum is non-confidential.

The Office Action points to col. 7, lines 5-8 of Saliba for this teaching. Appellants respectfully submit there is absolutely no teaching or suggestion in this portion, nor any other portion of Saliba, that teaches the claimed feature. Specifically, the relied upon portion of Saliba merely speaks to specialized functions in the context of electronic shopping.

In general, in a preferred embodiment of Saliba, a protocol is used to exchange information between an electronic commerce client application ("commerce client") which runs on the computer of a World Wide Web user, and an electronic commerce server application ("commerce server") which runs on a Web site. The protocol specifies a format for embedding a generic client-to-server function call within HTML (HyperText Markup Language) content such that a user can initiate the function call while viewing an HTML document via the standard Web browser. Specialized functions such as "get price," "get inventory," and "calculate tax" can thereby be placed within standard Web documents, such as electronic catalog documents used by online merchants to sell products. Client-to-server function calls are passed as HTTP POST

messages from the Web browser to the Web server; server-to-client function calls are passed as MIME messages returned to the Web browser. Because all information is passed using standard HTTP messages, end users can access the electronic commerce system from behind Internet firewalls that permit the passage of HTTP traffic.

The relied upon portion of Saliba states:

...(iii) storing, encrypting and forwarding to the merchants payment (e.g., credit card) information, (iv) storing and providing to merchants address information for the shipping of goods, and (v) passing receipts for online purchases to an online banking application such as Microsoft Money.TM. or Quicken.RTM..

Neither this portion, nor any other portion of Saliba, makes any reference whatsoever to functionality nor componentry that is capable of determining whether data is confidential or not, and performing encryption on the confidential information.

Secondly, independent claims 44 and 45 are directed toward communicating the information where, for example, the first datum is communicated with encryption and the second datum is communicated without encryption.

The Office Action references Col. 1, lines 33-38 of Saliba, as well as columns 4 and 7, for this teaching. One of the identified portions Saliba states:

These hypertext documents, which are created using HTML (the Hypertext Markup Language), contain the various product offerings and other purchase-related information of the respective merchants, and typically include forms for allowing consumers to return payment and address information to the merchants. One significant problem with this approach is that the existing World Wide Web components (e.g., HTTP, HTML, and existing standard Web browsers) are not well suited for performing general purpose client-server transactions over the Internet, making it difficult to migrate commerce-related functionality to the client (consumer) side.

Column 4 of Saliba discusses common definitions of the internet, client-server, etc, and the relied upon portion of column 7 is reproduced above.

However, Saliba makes no mention nor provides any functionality or componentry in either these sections nor any other section that anticipates or renders obvious the claimed feature.

As a matter of fact, Saliba only mentions "encryption" twice. Once in the paragraph beginning at the bottom of col. 6:

In the context of electronic shopping, these specialized functions may include various services for facilitating the analysis of merchant offerings and the placement of product orders. For example, the commerce client 132 may include functionality for (i) storing product information (including information

contained within HTML documents viewed via the browser 112) from multiple merchants for subsequent recall and use, (ii) providing a mechanism to facilitate user comparison of information on like products from different merchants, (iii) storing, *encrypting* and forwarding to the merchants payment (e.g., credit card) information, (iv) storing and providing to merchants address information for the shipping of goods, and (v) passing receipts for online purchases to an online banking application such as Microsoft Money.TM. or Quicken.RTM.. Similarly, the commerce server 136 may include functionality for (i) retrieving product information (such as price and inventory) not contained within the merchant's HTML documents, (ii) capturing and processing orders from users, and (iii) calculating sales taxes and shipping and handling costs. The addition of such functionality (particularly on the client side) would provide considerable benefits over existing commerce systems. (Emphasis Added)

and again in Table 2 on col. 11: (Emphasis Added)

# 11

TABLE 2

Method	Description
AddLineItem	Adds line item (stock keeping unit number, description, image, etc.) to shopping basket. Can be invoked by the user while viewing an HTML catalog page.
SubmitOrder	Takes all items saved in the shopping basket, requests payment information, <i>encrypts</i> the payment and shopping basket information, and then sends the <i>encrypted</i> information to the Merchant Server. Can be invoked by the user while viewing the contents of the shopping basket.
ShowWallet	Displays to the user the contents of the Wallet.
ShowAddressBook	Displays to the user the contents of the Address Book.
ModifyWallet	Pops up a dialogue that allows the user to add/delete/modify credit card and other payment information.
ModifyAddressBook	Pops up a dialogue that allows the user to add/delete/modify addresses stored within the address book.
ViewBasket	Builds an HTML file from the items currently stored within the shopping basket, and then passes the HTML file to the browser for display.
ViewHistory	Builds an HTML file from the items currently stored within a history file, and then passes the HTML file to the browser for display. Allows merchants to add a button that lets the consumer jump from a catalog page to a list of the items that have been purchased from the merchant.
DeleteItem	Removes a user-selected item from the shopping basket while the user is viewing the contents of the basket.
UpdateOrderInfo	Saves into the basket information that is common to a set of line items from the same merchant (e.g., tax and S/H charges). Invoked, for example, when the user selects an "UPDATE" button to obtain detailed pricing information on the entire shopping basket.

Clearly, no reasonable interpretation of either of these portions of Saliba, nor any other portion of Saliba, would lead one to conclude the claimed features of determining which data is confidential, and encrypting the confidential data were anticipated.

In complete contrast to an exemplary advantage of the claimed invention, which is to reduce the amount of unnecessarily encrypted data and thus processor load (see pg. 2, lines 7 – 10), Saliba reveals in relation to the “SubmitOrder” functionality in Table 2 that the exact situation in which Appellants are trying to avoid is practiced - the encryption of information, i.e., the shopping basket information, that is not confidential.

Moreover, and in contrast to and teaching away from the claimed invention, Saliba actually specifically states “Because *all information is passed using standard HTTP messages*, end users can access the electronic commerce system from behind Internet firewalls that permit the passage of HTTP traffic.” (Emphasis Added) Again, this is a clear indication that in Saliba there is no teaching or suggestion of communicating the information based on an identification such that, for example, the first datum is communicated with encryption and the second datum is communicated without encryption.

Additionally, Saliba is addressing an entirely different problem than the claimed invention. As discussed, for example, in Appellants specification, flagged portions of web pages are encrypted while same portion of the same web page are not encrypted, or vice versa.

In complete contrast, Saliba addresses:

...the problem of performing commerce-related transactions over the Internet involves the use of specialized client and server software components which communicate with one-another using some transport protocol other than HTTP. This approach, which is used by the version 1.0 electronic commerce system of eShop Inc., generally requires the use of some dedicated TCP/IP port other than port 80, which is reserved for HTTP. (TCP/IP is a low level Internet communications protocol which uses port definitions to route messages to applications.) Unfortunately, many company networks have Internet firewalls (i.e., systems which restrict traffic into and/or out of the company network to provide network security) which block traffic on TCP/IP ports other than port 80 (and possibly a few other reserved ports), preventing consumers from using such electronic commerce systems from their computers at work. Additionally, systems of this type do not take advantage of the widespread use by potential consumers of the World Wide Web.

At least based on these differences, independent claims 44 and 45 are not anticipated by Saliba.

Dependent Claim 4 recites that the first and datum are communication in a message and wherein the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum comprise the step of employing a same path between the first computing device and the second computing device to communicate the first datum with encryption and the second datum without encryption.

Since Saliba fails to communicate the first datum of the message with encryption and communicate the second datum of the message without encryption, Saliba also fails to anticipate employing the same path as claimed.

Dependent Claim 5 recites that the step of employing the same path to communicate the first datum with encryption and the second datum without encryption comprises the step of employing a TCP/IP passage between the first computing device and the second computing device to communicate the first datum with encryption and the second datum without encryption.

Since Saliba fails to communicate the first datum of the message with encryption and communicate the second datum of the message without encryption, Saliba also fails to anticipate employing a TCP/IP passage between the first computing device and the second computing device to communicate the first datum with encryption and the second datum without encryption as claimed.

Dependent Claim 10 recites wherein the Web page comprises hypertext markup language, wherein the first datum comprises the credit card number, wherein the second datum comprises information related to a purchase by the user, wherein the program is embedded in the Web page, and further comprising loading the program on the first computing device after the Web page is received by the first computing device. Dependent Claim 11 recites wherein the step of communicating the procedure from the second computing device to the first computing device comprises the step of selecting the procedure to comprise a procedure based on a machine independent Web protocol.

In that Saliba provides no functionality that can be equated to the claimed program, Saliba fails to anticipate the features of claims 10 and 11.

Dependent Claim 18 recites the first and second datum are communication in a message and wherein the first computing device employs a same path to receive from the second computing device, the first datum of the message with encryption and the second datum of the message without encryption. Dependent claim 19 recites that the same path comprises a TCP/IP passage between the first computing device and the second computing device.

As discussed above, since Saliba fails to teach or suggest the first datum of the message with encryption and the second datum of the message without encryption, Saliba can not anticipate the features of claims 18 and 19.

Dependent Claim 23 recites that the first and datum are communication in a message and wherein the second computing device employs the procedure to encrypt the first datum for communication of the first datum of the message from the second computing device to the first computing device. Dependent Claim 24 recites that the procedure is based on a machine independent Web protocol.

As discussed above, in that Saliba fails to teach or suggest any feature that can be equated to the claimed procedure, Saliba also fails to anticipate claims 23 and 24.

Dependent Claim 26 recites that the first and datum are communication in a message and wherein the procedure causes the second computing device to select the first datum for communication of the first datum of the message from the second computing device to the first computing device with encryption of the first datum.

Saliba makes no mention of the procedure as claimed nor the encryption of the first datum.

Dependent Claim 27 recites that the procedure causes the second computing device to select the second datum for communication of the second datum of the message from the second computing device to the first computing device without encryption of the second datum. Saliba makes no mention of the procedure as claimed nor the selection of the second datum for communication of the second datum of the message from the second computing device to the first computing device without encryption of the second datum.

Dependent Claim 28 recites an article of manufacture comprising at least one computer usable medium having computer readable program code operable to perform the steps of claim 44.

Since Saliba does not anticipate claim 44, Saliba also does not anticipate claim 28 for at least the above reasons and the additional features recited therein.

Dependent Claim 29 recites that the first datum is confidential information to a user and the second datum is non-confidential information to the user.

In that Saliba fails to disclose the term "confidential," or provide any delineation between types of data, Saliba fails to anticipate claim 29.

Dependent Claim 30 recites that the first and second datum are communication in a message and further comprising:

receiving the input information from a user, the input information comprising a plurality of input fields; and

determining each input field comprising confidential information to the user and each input field comprising non-confidential information to the user, wherein the first datum is confidential information and the second datum is non-confidential information.

Saliba has no capability to determine confidential or non-confidential information. To the contrary, as stated in Table 2 of Saliba, the payment and shopping basket information are encrypted.

Dependent Claim 32 recites that the communicating steps comprise:

encrypting the information in each of the input fields identified as comprising confidential information; and

not encrypting the information in each of the input fields identified as comprising non-confidential information.

Saliba fails to teach or suggest the claimed encrypting and not encrypting steps as claimed.

Dependent Claim 33 recites that the Web page comprises hypertext markup language, wherein the first datum comprises the credit card number, wherein the second datum comprises

information related to a purchase by the user, wherein the procedure is in an applet received from the second communication device.

Saliba fails to teach or suggest the claimed features and particularly the claimed applet and corresponding functionality.

Dependent Claim 34 recites that the first datum is communication in a message, wherein the first computing device is operable to receive the input information from a user, the input information comprising a plurality of input fields, and determine each input field comprising confidential information to the user and each input field comprising non-confidential information to the user, wherein the first datum is confidential information and the second datum is non-confidential information.

Saliba has no capability of distinguishing between confidential and non-confidential information.

Dependent Claim 35 recites that the first computing device encrypts the information in each of the input fields identified as comprising confidential information and does not encrypt the information in each of the input fields identified as comprising non-confidential information.

Saliba fails to teach or suggest the claimed encrypting and not encrypting steps as claimed.

Claims 4-5, 10-11, 18-19, 23-24, 26-30, 32-35 and 44-45 are clearly patentably distinguishable and not anticipated by Saliba.

**Whether claims 2, 13-14, 16, 31 and 36-43 are obvious under 35 U.S.C. §103(a) in view of Saliba and Ice (U.S. Patent 6,589,031).**

Ice is relied upon in that the Office Action concedes that "Saliba is silent on the capability of having steps (d) and (e) occur at least substantially simultaneously."

Appellants would like to initially point out that Ice *is not* Prior Art. Appellants' filing date is November 8, 1999 – which is before the June 31, 2000 filing date of Ice.

Nevertheless, Ice is directed toward an apparatus and method for routing encrypted transaction card identifying data through a public telephone network. A personal computer transmits encrypted information identifying a transaction card, together with a serial number of

an encryption unit in which the information was encrypted, over a public network to a payment server. The payment server generates a single-use credit card number, which is returned to the personal computer over the public network, and stores the single-use credit card number together with the serial number and the encrypted information. The personal computer then transmits the single-use credit card number to a merchant's server through which a transaction is to be made. The single-use credit card number is transmitted to the payment server, which is identified according to a portion of the single-use credit card number. The payment server then decodes a portion of the encoded information according to a cryptogram located within a data base according to the serial number stored with the single-use credit card number. The payment server then transmits decoded information allowing the transaction to proceed.

In Ice, the routing of a transaction card together with a serial number of an encryption unit is discussed. Ice States: "at this point, the data transferred from the personal computer 14 the payment server 34 includes both encrypted information identifying the credit card number and unencrypted information specifying the serial number of the encryption unit 26 and the address to which the transaction is to be billed."

The credit card number of Ice is however *not* a user input field in that *the payment server* 34 generates the single-use credit card number.

Additionally, it is unclear where the Office finds support for the claimed steps occurring "substantially simultaneously" as asserted, in that Ice merely discloses transferring information.

Based at least on the above, each of claims 2, 13-14, 16, 31 and 36-43 are independently patentable.

**Whether claims 3 and 17 are obvious under 35 U.S.C. §103(a) in view of Saliba and Trcka (U.S. Patent Publication 2001/0039579).**

The Office Action concedes that Saliba is silent "on the capability of communicating the first datum with encryption in a first packet of the message; and communicating the second data without encryption in a second packet of the message different from the first packet of the message."

Claim 3 recites that the first and datum are communication in a message and wherein the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum comprise the steps of:

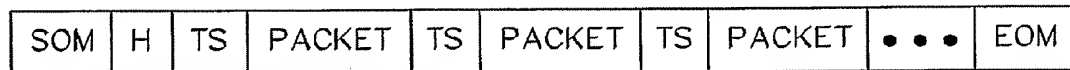
communicating the first datum with encryption in a first packet of the message;

and

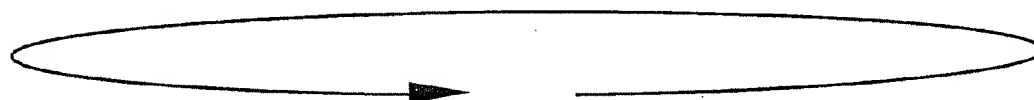
communicating the second datum without encryption in a second packet of the message different from the first packet of the message.

Claim 17 recites that the first and datum are communication in a message and wherein the first computing device receives the first datum with encryption in a first packet of the message, and wherein the first computing device receives the second datum without encryption in a second packet of the message different from the first packet of the message.

Fig. 6A (reproduced below) and paragraphs 92 and 93 are evidently relied upon for this teaching.



*FIG. 6a*



*FIG. 6b*

### KEY

SOM = START OF MEDIA  
 H = MEDIA HEADER  
 TS = TIME/DATE STAMP  
 EOM = END OF MEDIA

[0092] FIG. 6(a) illustrates, for one implementation of the Archival Data Processing Module 90, the format used for recording the archival data stream to a tape or other storage medium of the Archival Media Unit 80. The recording begins with a start-of-media marker, followed by a media header. The media header may include, for example, an identifier of the network 30 from which the recording was generated, and an identifier of an authorized user that was logged into the system 60 when the recording was initiated. The media header is followed by a chronological sequence of the encrypted (or unencrypted) packets and their respective date/time stamps, followed by an end-of-media marker.

**[0093]** FIG. 6(b) illustrates a corresponding format used for storing the data stream to the Good-Data Cyclic Recorder 82. The same format may also be used for storing traffic data to the Bad-Data Cyclic Recorder 84. As illustrated, the cyclic recording format is similar to the Archival Media Unit 80 recording format, with the exception that the start-of-media, media header, and end-of-media fields are omitted. As represented by the arrow in the drawing, the recorded data is overwritten on a circular basis (i.e., the oldest data is overwritten first).

Trcka merely indicates that the header can be followed by a sequence of encrypted *or* unencrypted packets.

Neither this portion of Trcka nor any other portion teach or suggest the claimed communicating of the first datum with encryption in a first packet of the message; and the communicating of the second datum without encryption in a second packet of the message different from the first packet of the message.

In that the cited references, either alone or in combination, fail to teach each and every feature of the claims, claims 3 and 17 are patentably distinguishable therefrom.

**Whether claims 6, 8-9 and 21-22 are obvious under 35 U.S.C. §103(a) in view of Saliba and Schneier.**

The Office Action concedes that “Saliba is silent on the capability of employing a second key to decrypt the first datum of the message and the first and the second key comprised a matched key to communicate the encrypted data.”

Schneier fails to overcome the deficiencies of Saliba.

Dependent claim 6 recites that the first and second datum are communication in a message and wherein the step of communicating the first datum of the message with encryption of the first datum comprises the step of employing a key to encrypt the first datum of the message for communication of the first datum from the first computing device to the second computing device with encryption of the first datum.

Dependent claim 8 recites that the key comprises a first key and further comprising the step of employing a second key to decrypt the first datum of the message after communication of the first datum from the first computing device to the second computing device with encryption of the first datum.

Dependent claim 9 recites further comprising the step of selecting the first key and the second key to comprise matched keys for communication of the first datum of the message from the first computing device to the second computing device with security of the first datum.

Dependent claim 6 recites that the key comprises a first key, and wherein the first computing device employs a second key to decrypt the first datum of the message communicated from the second computing device to the first computing device with encryption of the first datum.

Dependent Claim 22 recites that the first computing device selects the first key and the second key to comprise matched keys for communication of the first datum of the message from the second computing device to the first computing device with security of the first datum.

The Office Action states that Schneier "discloses communications using symmetric cryptography where the second key is used to decrypt the encrypted message (page 28, item (5)), and the first (page 28, item (3)), and second key comprised a matched key (page 28, item (5)), to communicate the encrypted data."

The relied upon portion of Schneier illustrates:

28

CHAPTER 2 *Protocol Building Blocks*

## 2.2 COMMUNICATIONS USING SYMMETRIC CRYPTOGRAPHY

How do two parties communicate securely? They encrypt their communications, of course. The complete protocol is more complicated than that. Let's look at what must happen for Alice to send an encrypted message to Bob.

- (1) Alice and Bob agree on a cryptosystem.
- (2) Alice and Bob agree on a key.
- (3) Alice takes her plaintext message and encrypts it using the encryption algorithm and the key. This creates a ciphertext message.
- (4) Alice sends the ciphertext message to Bob.
- (5) Bob decrypts the ciphertext message with the same algorithm and key and reads it.

What can Eve, sitting between Alice and Bob, learn from listening in on this protocol? If all she hears is the transmission in step (4), she must try to cryptanalyze the ciphertext. This passive attack is a ciphertext-only attack; we have algorithms that are resistant (as far as we know) to whatever computing power Eve could realisti-

Items 3 and 5 merely illustrate encryption of a plaintext message into a ciphertext message and decrypting the message in step 5 with the same algorithm and key.

Schneier fails to overcome the deficiencies of Saliba. In that the cited references either alone or in combination teach each and every claimed feature, each of claims 6, 8-9 and 21-22 are patentably distinguishable therefrom.

**Whether claims 7 and 20 are obvious under 35 U.S.C. §103(a) in view of Saliba and Chang (U.S. Patent 6,105,021).**

Dependent claim 7 further comprises the step of communicating a key from the second computing device to the first computing device, and wherein the step of communicating the first datum of the message from the first computing device to the second computing device with encryption of the first datum comprises the step of employing the key to encrypt the first datum of the message for communication of the first datum from the first computing device to the second computing device.

Dependent claim 20 recites that the first and datum are communication in a message and wherein the information communicated from the first computing device to the second computing device includes a key employed by the second computing device to encrypt the first datum of the message for communication of the first datum from the second computing device to the first computing device.

Chang fails to overcome the deficiencies of Saliba. In that the cited references either alone or in combination teach each and every claimed feature, each of claims 7 and 20 are patentably distinguishable therefrom.

**Whether Claims 28 and 39 are in compliance with 35 U.S.C. §101.**

Claim 28 recites an article of manufacture comprising at least one computer usable medium having computer readable program code operable to perform the steps of claim 44.

Claim 39 recites computer readable medium comprising instructions to perform the steps of claim 36.

The Office Action indicates the above claims are non-statutory in that that they “lack the necessary physical articles or objects to constitute a machine or manufacture within the meaning of 35 USC 101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter... They are, at best, functional descriptive material per se.”

A computer-readable medium encoded with a computer program is an article of manufacture - indistinguishable from any other component, hardware or software which may be associated with a computer to control its functionality. Machine-executable computer programs include signals which are read from the computer-readable media for controlling the operation of a computer. Such a computer readable media does not fit within any category of judicially-created exceptions to 35 U.S.C. § 101 – and is clearly a physical article(s).

35 U.S.C. § 101 defines patentable subject matter as “any new and useful process, machine, manufacture or composition of matter, or any new and useful improvement thereof.” The Supreme Court has stated that, in enacting § 101, Congress had intended that it “include anything under the sun that is made by man.” *Diamond v. Chakrabarty*, 447 U.S. 303, 309, 206 USPQ 193, 197 (1980), quoting S. Rep. No. 1979, 82d Cong., 2d Sess., 5 (1952);, H.R. Rep. No. 1923, 82d Cong., 2d Sess., 6 (1952), also reiterated in *Diamond v. Diehr*, 450 U.S. 175, 209 USPQ 1 (1981). The Supreme Court also recognized that there were exceptions to this sweeping statement. Excluded from patentability is subject matter in the categories of “laws of nature, physical phenomena, and abstract ideas.” *Diehr*, 450 U.S. at 185, 209 USPQ at 7 (1981).

A claimed invention can only be excluded from patent protection under §101 if it falls into a judicially created exception to §101. Appellants respectfully submit this is not the case and both claims 28 and 39 are in full compliance with 35 U.S.C. §101.

Appln. No. 09/435,736

Attorney Docket No. 4366-41

For at least the above reasons, Appellants respectfully submit that the application is in full compliance with all applicable rules and regulations, the claims are novel and non-obvious and that the application should be passed to Issuance.

Respectfully submitted,

SHERIDAN ROSS P.C.

By: \_\_\_\_\_

Jason H. Vick

Registration No. 45,285

1560 Broadway, Suite 1200

Denver, Colorado 80202-5141

(303) 863-9700

Date: \_\_\_\_\_

1 Aug '17